UNITED STATES DISTRICT COURT FOR THE WESTERN DISTIRCT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF DATA PREVIOUSLY EXTRACTED FROM GOOGLE ACCOUNT IDENTIFIER DRUMMOND330@GMAIL.COM CURRENTLY AT ATF ROANOKE LOCATED AT 310 FIRST ST. SW STE.500, ROANOKE, VA 24011	* * * * * * *	**Case No:** 7:23mj48

****

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Detective Marcus Talley, being duly sworn, hereby depose, and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—data previously extracted from Google Account Identifier Drummond330@gmail.com (Account) — which is currently in law enforcement possession, as described in Attachment A, and the extraction from that property of electronically stored information as described in Attachment B.

2. I have been employed by the Metropolitan Police Department (MPD) since May 20, 2013. In 2018, I was promoted to the rank of Detective where I am presently assigned as a Federal Task Force Officer with ATF. My current duties involve investigating and assisting in the prosecution of federal firearms violations, including the illegal possession and trafficking of firearms. During my time as a police officer, I have been assigned to the First District Detective's Unit, Narcotics and Special Investigations Division's Criminal Interdiction Unit, Narcotics and Special Investigations Division's Narcotics Enforcement Unit, the First District Crime Suppression

Team and the First District Uniform Patrol Division.

3. As an ATF Task Force member, I am an "investigative or law enforcement officer" of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other officers/agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that JONATHAN JOHNSON (JOHNSON) committed a violation of 18 U.S.C. § 922(g)(1) (Unlawful Possession of a Firearm and Ammunition by a Person Convicted of a Crime Punishable by Imprisonment for a Term Exceeding One Year). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, or fruits of these crimes further described in Attachment B.

IDENTIFICATION OF THE ACCOUNT TO BE EXAMINED

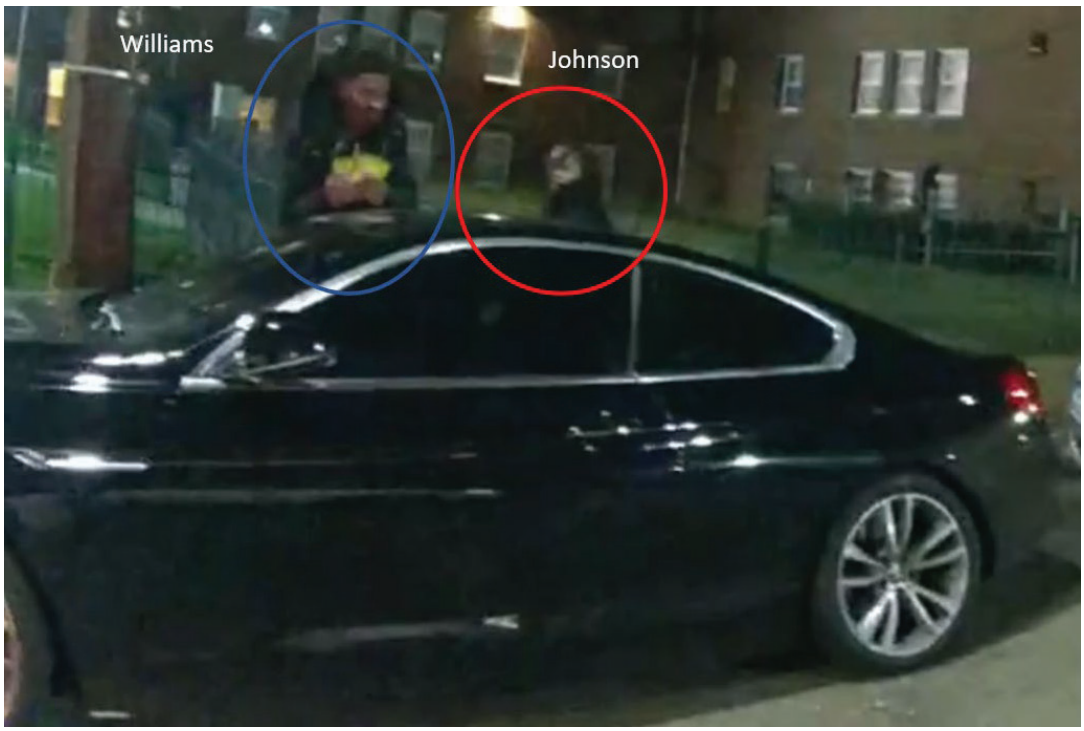
6. The property to be searched is data previously extracted from Google Account Identifier Drummond330@gmail.com (Account).

7. The data previously extracted from the Account is currently at ATF Roanoke located at 310 First St. SW Ste.500, Roanoke, VA 24011.

INVESTIGATION OF
JONATHAN JOHNSON

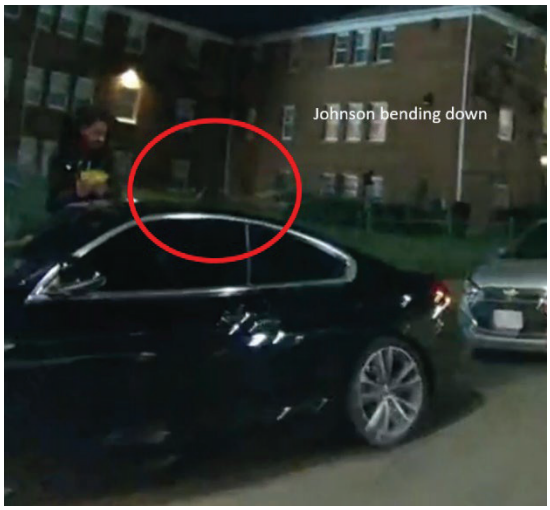
8. On January 12, 2021, JOHNSON was indicted in the District of Columbia for one count of 18 U.S.C § 922(g)(1). The indictment stems from JOHNSON's arrest on December 29, 2020.

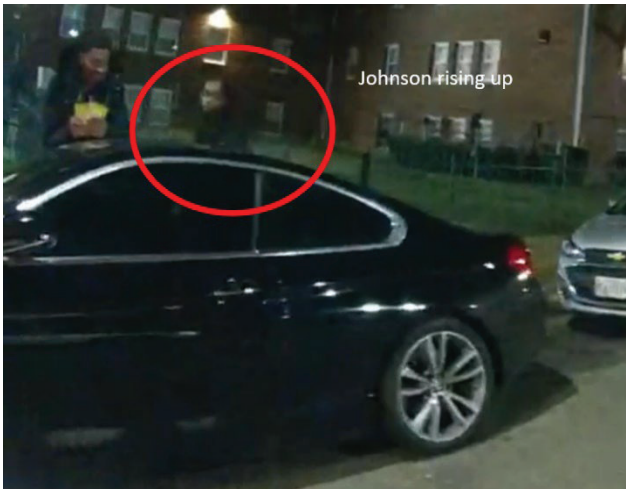
9. On that date, members of the Metropolitan Police Department (MPD) Seventh District Crime Suppression Team (7D CST) were on patrol in a vehicle when they observed two adult, African American males, identified as JOHNSON and GARY WILLIAMS (WILLIAMS), standing next to a parked BMW sedan (D.C. license plate number BCA129), in front of 3407 13th Place Southeast in Washington, D.C. At that time, the vehicle was parked such that the passenger side was closest to the curb and the driver's side was parallel to the flow of traffic.

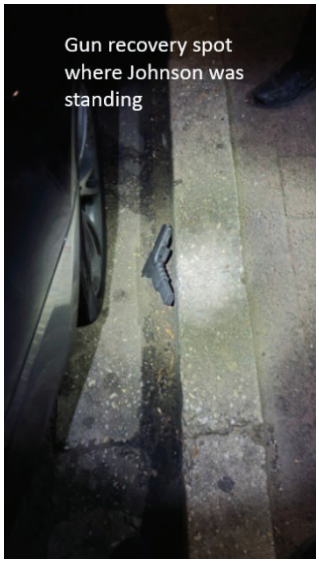


10. As the officers approached the parked BMW in their vehicle, they had their windows down and observed WILLIAMS leaning on the car's front passenger-door area, while JOHNSON

was standing toward the rear of the vehicle. As the officers approached, they noticed JOHNSON turn his body away from the police vehicle in a quick maneuver. When the officers drove closer, one officer observed JOHNSON crouch down at the back of the BMW, in front of the rear wheel-well of the car, and out of view of the officers, while WILLIAMS was standing upright with both hands visible and resting on the top of the car. The officers parked and exited their vehicle in order to make contact with JOHNSON who, seconds later, stood back up. After exiting their vehicle, the officers immediately approached and looked at the ground around the back wheel-well area of the vehicle, where the defendant was seen crouching. Officers immediately observed a firearm between the rear tire of the vehicle and the curb and placed JOHNSON under arrest.







11. Search incident to arrest, JOHNSON was in possession of the vehicle key for the BMW. A Washington Area Law Enforcement System (WALES) check for the registration of the vehicle confirmed that the vehicle was registered to Defendant Johnson.

12. A criminal history check of JOHNSON through the National Crime Information Center (NCIC) confirmed that the defendant has a prior felony conviction for Robbery While Armed and Possession of a Firearm during Crime of Violence in the Superior Court for the District of Columbia, case number 2008 CF3 27871. The defendant was sentenced to sixty (60) months of incarceration for this conviction. The defendant is currently on supervision for this conviction. Therefore, the defendant was aware at the time of his arrest in this case that he had prior convictions for crimes punishable by more than one year.

13. The recovered firearm was determined to be a Glock 23 handgun bearing serial number of BLFE271. When it was recovered, it was loaded with one (1) round in the chamber and twenty-one (21) rounds in a twenty-two (22) round high capacity magazine. Additionally, the firearm was equipped with a "giggle switch." This switch is a modification to the firearm after manufacturing which enables the firearm to switch from semi-automatic firing to fully automatic firing with a cross-

bolt type switch. When in fully automatic mode, the firearm will fire multiple bullets with only one pull of the trigger. There are no firearm or ammunition manufacturers in the District of Columbia. Therefore, the seized firearm and ammunition would have traveled in interstate commerce.

14. The recovered firearm and magazine were processed for forensic evidence. Specifically, separate swabs were taken from the giggle switch, the firearm, and the magazine. Those swabs were sent to the FBI forensic laboratory in Quantico, Virginia for DNA analysis and potential comparison with a buccal swab taken from JOHNSON.

15. The swabs from the giggle switch and magazine were found to contain a mixture of DNA from five or more individuals and thus the FBI determined, based on their standards and protocols, that they were not suitable for comparison.

16. The swab from the firearm was interpreted as containing Male DNA and originating from four individuals. The FBI determined that this was suitable for comparison. The forensic analyst determined that it is 1.5 trillion times more likely if JOHNSON and three unknown, unrelated people are contributors than if four unknown, unrelated people are contributors. This provides very strong support for JOHNSON's inclusion as a contributor of DNA on the firearm.

17. Of the DNA mixture on the swab from the firearm, it was predicted that JOHNSON contributed approximately 18% of the DNA. This was the third highest of the four contributors. The two contributors with higher percentages of DNA in the mixture contributed approximately 58% and 21% of the DNA, respectively.

INVESTIGATION OF JERMAINE DRUMMOND

18. On August 29, 2022, in the US District Court for the Western District of Virginia, JERMAINE DRUMMOND (DRUMMOND) pled guilty to two counts of aiding and abetting in making a false statement to a federal firearms licensee in connection with the acquisition of firearms

in violation of 18 U.S.C. §§ 922(a)(6), 924(a)(2). Specifically, according to the Agreed Statement of Facts, DRUMMOND–a convicted felon–used other non-prohibited persons to purchase firearms for him. One of those firearms was the Glock 23 handgun bearing serial number of BLFE271 that JOHNSON is alleged to have possessed on December 29, 2020.

19. ATF agents obtained several search warrants during the course of their investigation of DRUMMOND. Specifically, on September 28, 2021, a US Magistrate Judge in the US District Court for the Western District of Virginia signed search warrant number 21-mj-138 authorizing the search of the Account. A copy of the data extracted from the Account is currently at ATF Roanoke located at 310 First St. SW Ste.500, Roanoke, VA 24011.

BACKGROUND CONCERNING PROVIDER'S ACCOUNTS

20. Google LLC (PROVIDER) is the provider of the internet-based account identified by Drummond330@gmail.com.

21. PROVIDER provides its subscribers internet-based accounts that allow them to send, receive, and store emails online. PROVIDER accounts are typically identified by a single username, which serves as the subscriber's default email address, but which can also function as a subscriber's username for other PROVIDER services, such as instant messages and remote photo or file storage.

22. Based on my training and experience, I know that PROVIDER allows subscribers to obtain accounts by registering on PROVIDER's website. During the registration process, PROVIDER often asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate email address for backup purposes, a phone number, and in some cases a means of payment.

23. Typically, once a subscriber has registered an account, PROVIDER provides email

services that typically include folders such as an "inbox" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username. PROVIDER subscribers can also use that same username or account in connection with other services provided by PROVIDER.

24. In general, user-generated content (such as email) that is written using, stored on, sent from, or sent to a PROVIDER account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete an email, the email can remain on PROVIDER's servers indefinitely. Even if the subscriber deletes the email, it may continue to exist on PROVIDER's servers for a certain period of time.

25. Thus, a subscriber's PROVIDER account can be used not only for email but also for other types of electronic communication, including, but not limited to: instant messaging, photo and video sharing, voice calls, video chats, SMS text messaging; or social networking. Depending on user settings, user-generated content derived from many of these services is normally stored on PROVIDER's servers until deleted by the subscriber. Similar to emails, such user-generated content can remain on PROVIDER's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on PROVIDER's servers for a certain period of time. Furthermore, a PROVIDER subscriber can often store contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on PROVIDER's servers. Based on my training and experience, I also know that evidence of who controlled, used, and/or created a PROVIDER account may be found within such computer files and other information created or stored by the PROVIDER subscriber. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity.

26. Based on my training and experience, I know that providers such as PROVIDER also collect and maintain information about their subscribers, including information about their use of PROVIDER services. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. Providers such as PROVIDER also commonly have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as PROVIDER typically collect and maintain location data related to subscriber's use of PROVIDER services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.

27. Based on my training and experience, I know that providers such as PROVIDER also often collect information relating to the devices used to access a subscriber's account – such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by PROVIDER in order to track what devices are using PROVIDER's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment

Identity ("IMEI"). Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other PROVIDER accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the PROVIDER account.

28. PROVIDER also often allows its subscribers to access its various services through an application that can be installed on and accessed via cellular telephones and other mobile devices. This application is associated with the subscriber's PROVIDER account. In my training and experience, I have learned that when the user of a mobile application installs and launches the application on a device (such as a cellular telephone), the application directs the device in question to obtain a Push Token, a unique identifier that allows the provider associated with the application (such as PROVIDER) to locate the device on which the application is installed. After the applicable push notification service (*e.g.*, Apple Push Notifications (APN) or Google Cloud Messaging) sends a Push Token to the device, the Token is then sent to the application, which in turn sends the Push Token to the application's server/provider. Thereafter, whenever the provider needs to send notifications to the user's device, it sends both the Push Token and the payload associated with the notification (*i.e.*, the substance of what needs to be sent by the application to the device). To ensure this process works, Push Tokens associated with a subscriber's account are stored on the provider's server(s). Accordingly, the computers of PROVIDER are likely to contain useful information that may help to identify the specific device(s) used by a particular subscriber to access the subscriber's PROVIDER account via the mobile application.

29. Based on my training and experience, I know that providers such as PROVIDER use cookies and similar technologies to track users visiting PROVIDER's webpages and using its

products and services. Basically, a "cookie" is a small file containing a string of characters that a website attempts to place onto a user's computer. When that computer visits again, the website will recognize the cookie and thereby identify the same user who visited before. This sort of technology can be used to track users across multiple websites and online services belonging to PROVIDER. More sophisticated cookie technology can be used to identify users across devices and web browsers. From training and experience, I know that cookies and similar technology used by providers such as PROVIDER may constitute evidence of the criminal activity under investigation. By linking various accounts, devices, and online activity to the same user or users, cookies and linked information can help identify who was using a PROVIDER account and determine the scope of criminal activity.

30. Based on my training and experience, I know that PROVIDER can maintain records that can link different PROVIDER accounts to one another, by virtue of common identifiers, such as common email addresses, common telephone numbers, common device identifiers, common computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple PROVIDER accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular PROVIDER account.

31. Based on my training and experience, I know that subscribers can communicate directly with PROVIDER about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as PROVIDER typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the

crimes under investigation because the information can be used to identify the account's user or users.

32. In summary, based on my training and experience in this context, I believe that the computers of PROVIDER are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved email for PROVIDER subscribers), as well as PROVIDER-generated information about its subscribers and their use of PROVIDER services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide PROVIDER with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

33. As explained above, information stored in connection with a PROVIDER account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a PROVIDER account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by PROVIDER can show how and when the account was accessed or used. For example, providers such as PROVIDER typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the

logged IP addresses, investigators can understand the chronological and geographic context of the PROVIDER account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculpate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the PROVIDER account may indicate its user's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).[1]

34. Based on my training and experience, I know that evidence of who controlled, used, and/or created a PROVIDER account may be found within the user-generated content created or stored by the PROVIDER subscriber. This type of evidence includes, for example, personal correspondence, personal photographs, purchase receipts, contact information, travel itineraries, and other content that can be uniquely connected to a specific, identifiable person or group. In addition, based on my training and experience, I know that this type of user-generated content can provide crucial identification evidence, whether or not it was generated close in time to the offenses under investigation. This is true for at least two reasons. First, people that commit crimes involving electronic accounts (*e.g.*, email accounts) typically try to hide their identities, and many people are

[1] At times, internet services providers such as PROVIDER can and do change the details and functionality of the services they offer. While the information in this section is true and accurate to the best of my knowledge and belief, I have not specifically reviewed every detail of PROVIDER's services in connection with submitting this application for a search warrant. Instead, I rely upon my training and experience, and the training and experience of others, to set forth the foregoing description for the Court.

more disciplined in that regard right before (and right after) committing a particular crime. Second, earlier-generated content may be quite valuable, because criminals typically improve their tradecraft over time. That is to say, criminals typically learn how to better separate their personal activity from their criminal activity, and they typically become more disciplined about maintaining that separation, as they become more experienced. Finally, because email accounts and similar PROVIDER accounts do not typically change hands on a frequent basis, identification evidence from one period can still be relevant to establishing the identity of the account user during a different, and even far removed, period of time.

AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

25. Because forensic examiners will be conducting their search of the extraction from the Account in a law enforcement setting over a potentially prolonged period of time, I respectfully submit that good cause has been shown, and therefore request authority, to conduct the search at any time of the day or night.

CONCLUSION

26. I submit that this affidavit supports probable cause for a warrant to search the data previously extracted from the Account described in Attachment A and to seize the items described in Attachment B.

Detective Marcus Talley
Metropolitan Police Department

Subscribed and sworn by telephone pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on May 3, 2023

Robert S. Ballou

The Honorable Robert S. Ballou
United States District Judge